Identity Theft and Online Fraud

IRS Efforts to Protect Taxpayers

Privacy, Governmental Liaison and Disclosure
May 9, 2012

Today's presentation

- How identity theft is a threat to the taxpayer
- What IRS is doing to address tax-related identity theft
- Identity theft detection and prevention
- Identity Protection PIN initiative
- Victim protection and assistance
- Combating online fraud
- How to protect yourself and your clients from identity theft

A persistent threat to American taxpayers

- Identity theft is the number one consumer complaint reported to the FTC
- Incidents related to government benefits are
  - most common
  - more complex
  - more time and money to detect and resolve
- IRS has seen an increase in refund fraud schemes in general and those involving identity theft in particular

How can identity theft affect taxes?

- Scenario 1: refund-related crime
  - Identity thief uses stolen SSN to file forged tax return and obtain refund early in the filing season
- Scenario 2: employment-related crime
  - Identity thief uses a stolen SSN to obtain employment

IRS response

- Identity theft is a top priority for the IRS
- We understand this is a frustrating situation for victims
- We are committed to improving our identity protection programs

Combating tax-related identity theft

- Goal: prevent identity theft and detect refund fraud *before* it occurs and to assist taxpayers who are victims
- Actions: enhanced fraud protection processes for the 2012 filing season
- Developed comprehensive identity theft strategy focused on:
  - Detection and prevention
  - Protection
  - Victim assistance

2012 filing season enhancements

- Developed filters to stop first-time perpetrators
- Marked decedent SSNs as a locking mechanism to prevent future misuse by identity thieves
- Developed Error Resolution Code to identify and stop fraudulent returns when it appears decedent SSNs are being misused
- Enhanced functionality of the Identity Protection PIN and expanded population to receive it

IRS detection efforts

- Placing identity theft indicators on taxpayer accounts to track and manage identity theft incidents
- Using business filters to ensure we accept legitimate returns and reject false returns
- Identifying and investigating refund fraud

What do identity theft indicators do?

- Primarily they identify different types of identity theft related to a specific account
  - Refund-related identity theft
  - Employment-related identity theft
  - Accounts with no filing requirement
  - Lost information (i.e., wallet)

What else do identity theft indicators do?

- *Prevent* victims from facing the same problems every year
- *Identify and track* tax-related identity theft problems
- *Distinguish* legitimate tax returns from fraudulent returns
- *Measure* the problem, monitor victims' accounts and develop processes to resolve problems

What do business filters do?

- Identify possible identity theft
- Ensure only legitimate returns are processed
- Flag questionable returns for manual review to validate legitimacy
- Reject fraudulent returns

IRS identity protection efforts

- Notifying taxpayers when identity theft has affected their tax accounts
- Issuing victims Identity Protection PINs

Identity Protection PIN

- IP PIN is a six-digit number assigned to taxpayers who:
  - Were identified as identity theft victims
  - Submitted required documentation
  - Had their account issues resolved
  - Filed a tax return for tax year 2010

What does the IP PIN do?

- Allows legitimate return to bypass identity theft filters
- Prevents processing of fraudulent returns
- Allows taxpayers to avoid delays in their federal tax return processing

Effect on tax administration

- If an IP PIN is issued to a taxpayer it must be used when the federal income tax return is filed
- Otherwise, the return will reject, potentially causing delays in processing

Key IP PIN information

- The IP PIN is specific to the tax year
- A new IP PIN issued every year
- The IP PIN should not be confused with the electronic signature ‘self-select’ PIN

What happens if IP PIN is required but not present?

- Electronic return will be rejected
- Taxpayer may request replacement
- Electronic return may be resubmitted with IP PIN
- If no IP PIN, paper return must be filed

IP PIN scenarios

- IP PIN issued to both taxpayers filing married filing jointly
  - Use only the IP PIN issued to taxpayer whose SSN is listed first

- Request extension and/or installment agreement

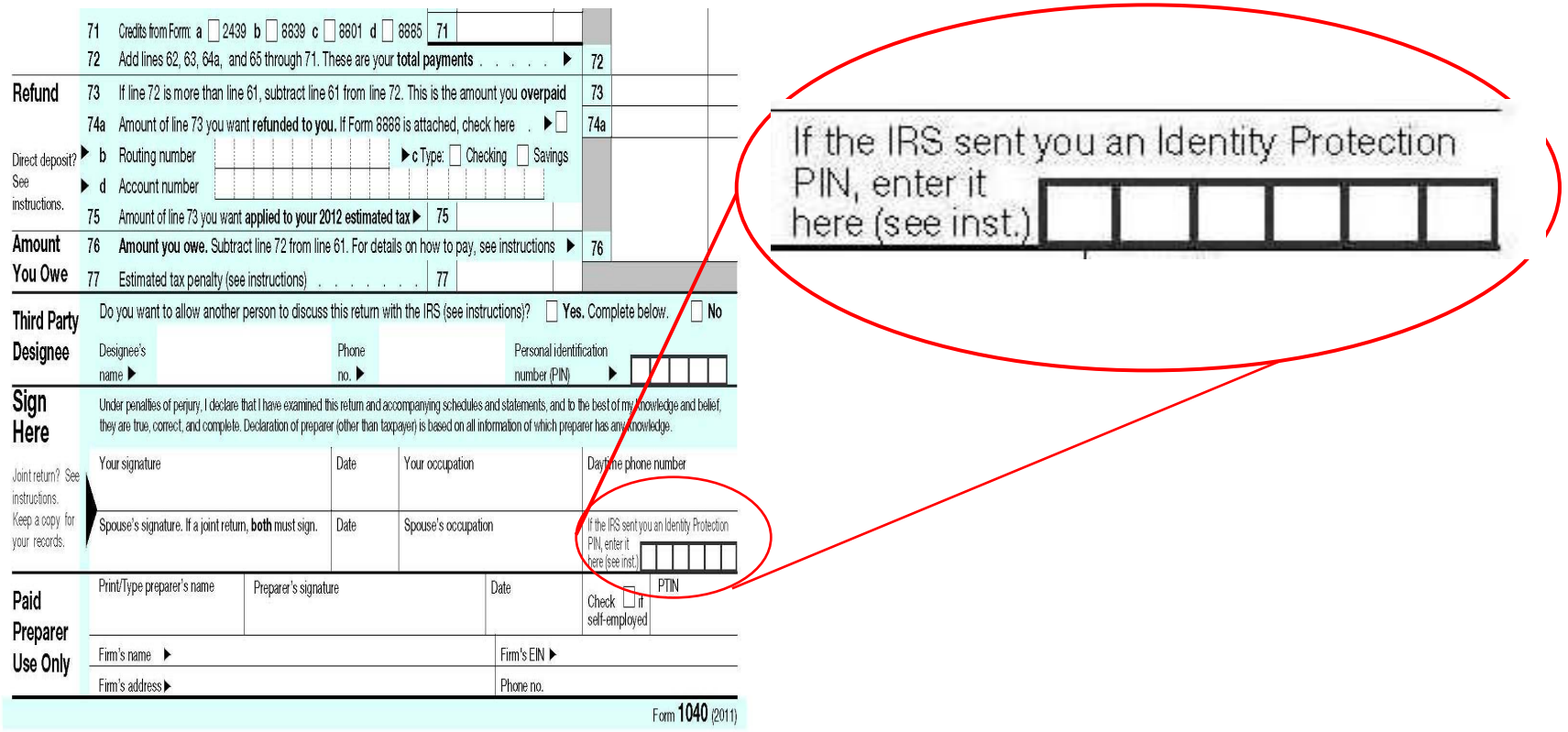
  Taxpayer must file paper request

Two notices for 2011 returns

- IP PIN Introductory Notice – Letter 4868CS
  - Mailed Mid-November 2011
  - Informed taxpayer IP PIN would be sent in December for use on 2011 return
- IP PIN Notice – IRS Letter 4869CS
  - Mailed Mid-December 2011
  - Provided single-use six-digit IP PIN

2011 Form 1040 Series Changes

Six boxes to right of spouse's occupation



IP PIN guidance for tax professionals for

- Ask your client if he received a letter from the IRS containing an IP PIN
- If so, input the IP PIN in the proper area
- Check with your software provider for the location for the IP PIN
- If your client says no letter with IP PIN received, continue preparation normally

IRS victim assistance efforts

- Speed up case resolution
- Provide more training for our employees who assist victims of identity theft
- Step up outreach and education of taxpayers so they can prevent and resolve tax-related identity theft issues quickly.

Identity Protection Specialized Unit

- IPSU is the central point of contact for taxpayers who are reporting their identity as stolen

  Toll-free number: 800-908-4490
  Monday - Friday, 7 a.m. - 7 p.m. local time

- Taxpayers can:
  - Self-report they are victims before it affects their tax accounts

IRS employee training

- Updated training for telephone representatives to ensure sensitivity when dealing with identity theft victims

- Developed training for employees who are not telephone assistors but interact with taxpayers or otherwise work identity theft cases

Taxpayer outreach

- Launched new section on IRS.gov dedicated to identity theft matters
- Issued identity protection messages throughout the filing season
- Educated return preparers about the IP PIN and identity theft
- Worked with software developers on inclusion of the IP PIN

How to help clients avoid identity theft

- Ensure they safeguard their personal information
- Instruct them to regularly check credit reports and other financial records
- Remind them the IRS does not initiate contact with taxpayers by email to request personal or financial information
  - This includes any type of electronic communication, such as text messages and social media channels

Actions your clients should take if they experience identity theft

- Contact their financial institutions and take appropriate action
- Contact the three credit bureaus to place a fraud alert and get free copies of credit reports
- File a police report with local law enforcement
- Contact the Federal Trade Commission: www.consumer.gov/idtheft/index.html

Actions your clients should take if they suspect they are the victim of tax related identity theft

- Contact the Identity Theft Specialized Unit
- Go to the IRS website and download Form 14039 *Identity Theft Affidavit*
- Submit the Form 14039 and all required documentation to the Identity Theft Specialized Unit

Identity theft resources

- Go to IRS.gov, scroll to the bottom of the homepage and click on ‘identity theft’
- IRS works closely with other organizations:
  - Federal Trade Commission
  - OnGuard Online
  - Identity Theft Resource Center

What about online identity theft?

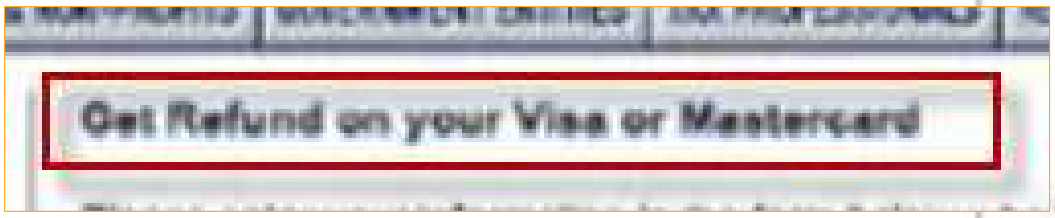
- Victims respond to online scams and unwittingly provide personal and financial information to phishers
  - **Phishing** – via the phishing Web form
  - **Malware** – by downloading malicious executable code
  - **Email** – via email (or money order)
  - **Vishing** – via the faxback form
  - **Stock** – via email (or wire transfer)

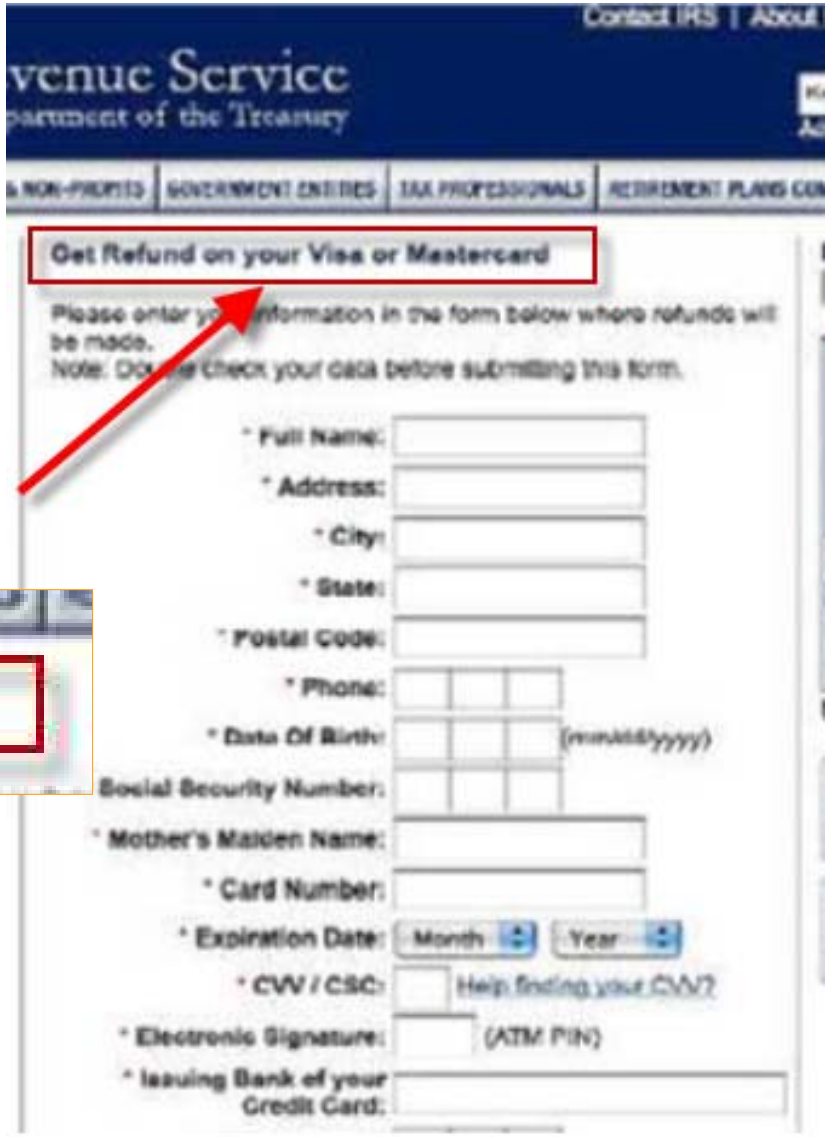
How Does the IRS mitigate online fraud?

- We work closely with registrars, hosting providers, free email providers and telecommunications providers to take the following actions:
  - De-register malicious domains
  - Remove malicious/fraudulent content
  - Suspend email accounts
  - Disable FAX numbers
  - Report unregistered securities entities

Phishing Website

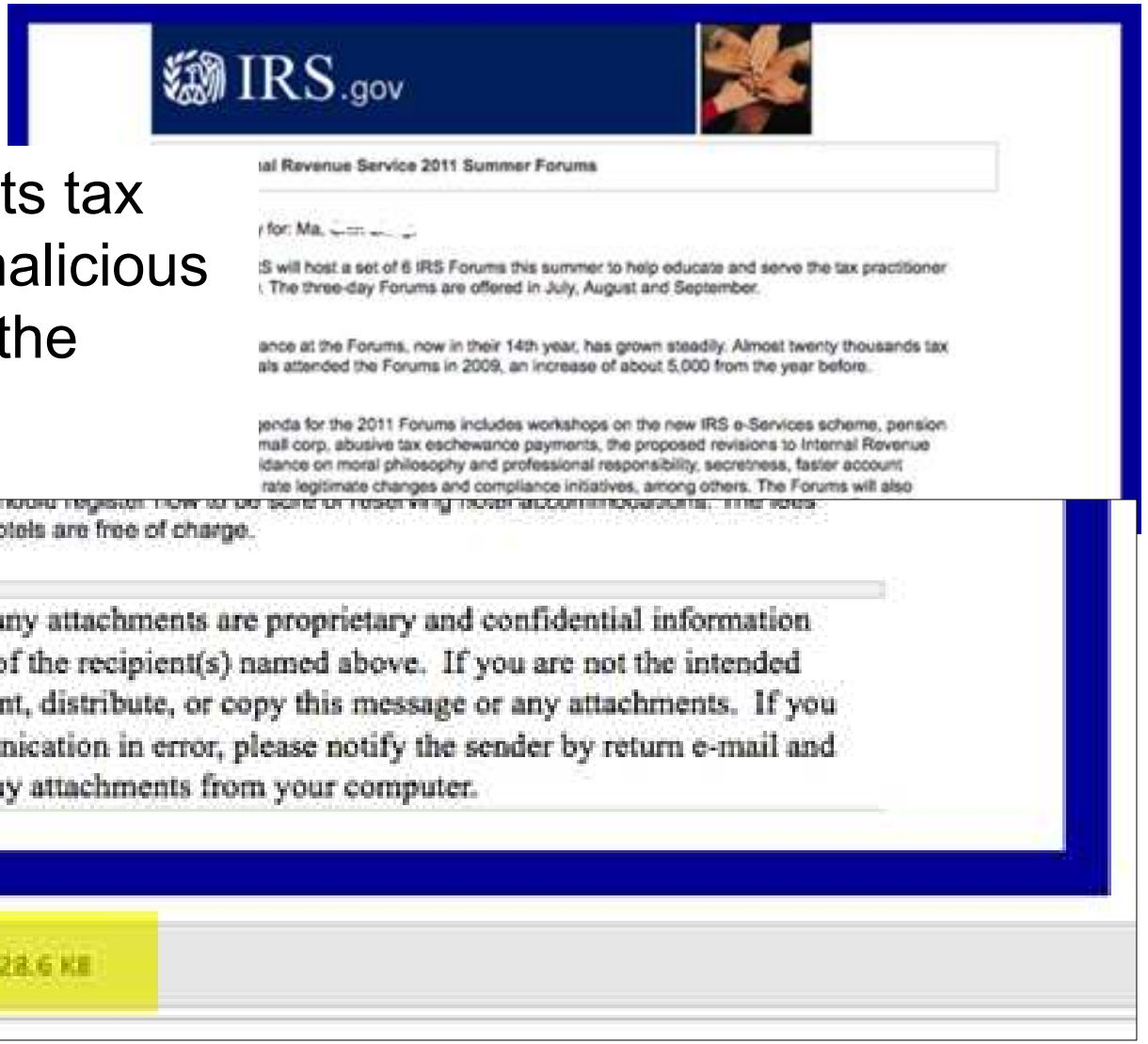
- This is an image of a typical IRS phishing webpage



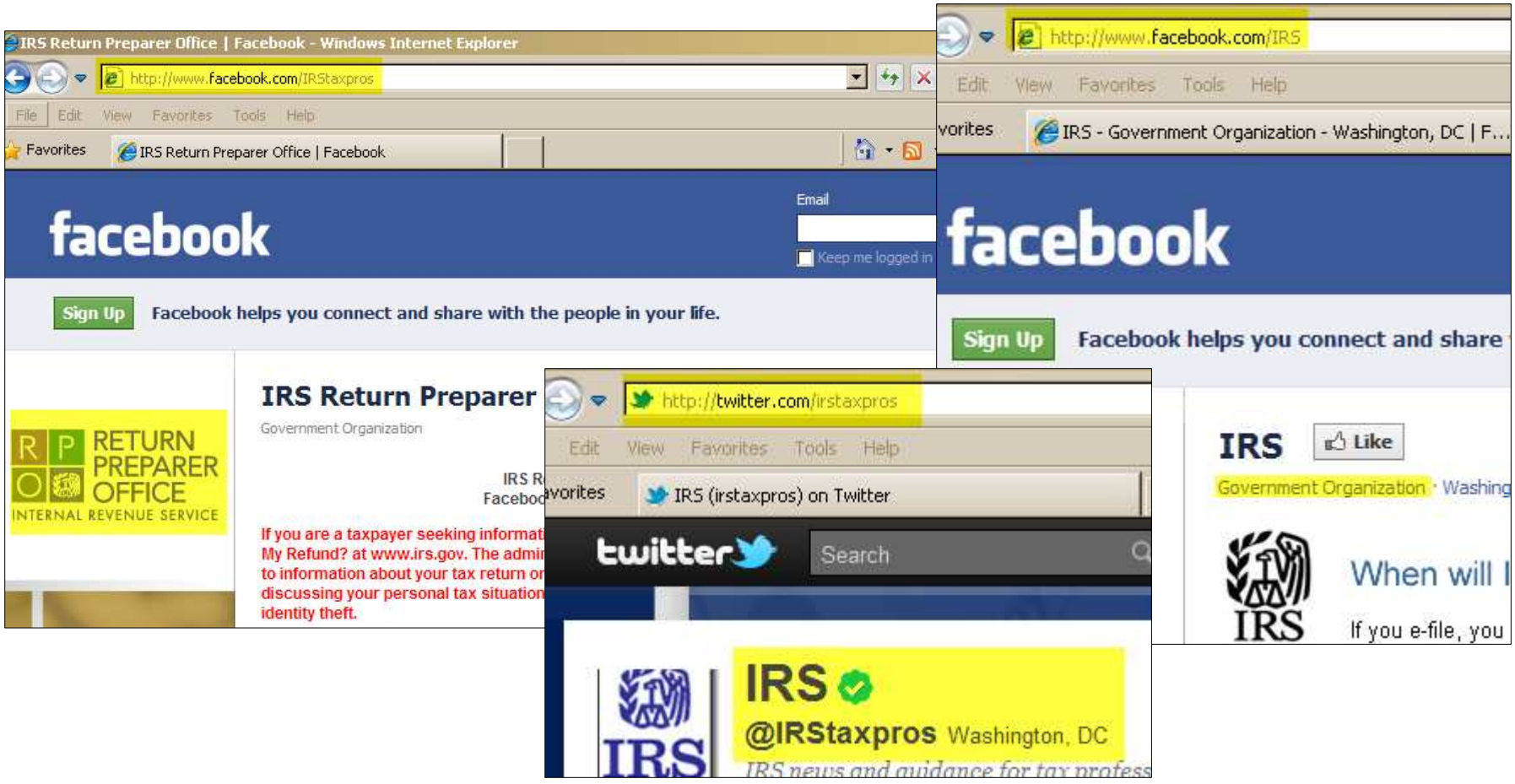


Malicious Email

This message targets tax practitioners -The malicious code is attached to the message



The IRS Uses Social Media Tools



If you or your client receive a suspicious IRS-related communication

- Report all unsolicited email claiming to be from the IRS to **phishing@irs.gov**
- Go to IRS.gov, scroll to the bottom of the homepage and click on ‘Report Phishing’

How to prevent online identity theft

- Watch out for phishing scams
- Secure your computer
- Always use strong passwords
- Limit the amount of personal information accessible by others
- Never answer ‘yes’ to pop-up screens

The IRS is committed to fighting identity theft

- Fighting identity theft will be an ongoing battle for the IRS
- The identity theft landscape is constantly changing, as identity thieves continue to create new ways of stealing personal information and using it for their gain

Conclusion

- This ends our formal presentation
- Thank you for participating
- Now we will answer some of your questions